



CLAIMS

We claim:

- 5 1. A system for sharing with multiple users and protecting content in the form of digital information from unauthorized access and/or use comprising:
 - a) content to be shared and protected; and
 - b) a permission wrapper having the ability to independently change the level of access to the content.
- 10 2. A server-less system for sharing and protecting content in the form of digital information from unauthorized access and/use comprising:
 - a. content to be shared and protected; and
 - b. a permission wrapper having the ability to independently change the level of access to the content.
- 15 3. The system according to Claim 1, wherein the permission wrapper includes embedded audit logs.
- 20 4. The system according to Claim 1, wherein the permission wrapper include audit logs which maintain a history of the access and initial use (i.e. viewed, printed, shared, etc.) to the content.
- 25 5. The system according to Claim 1, wherein the permission wrapper collects information on who, when, where and what the user did with the content.
6. The system according to Claim 1, wherein the permission wrapper tracks version control of the content.

7. The system according to Claim 1, wherein the permission wrapper includes embedded controls for controlling the use and sharing of the digital information content.
- 5 8. The system according to Claim 1, wherein the permission wrapper includes embedded controls containing inheritance rules which limit access to the content as defined by the original content provider.
9. The system according to Claim 1, wherein the embedded controls include multi-level
10 permission controls.
10. The system according to Claim 1, wherein the embedded controls can provide different access to the content by a designated class of users.
- 15 11. The system according to Claim 1, wherein the permission wrapper includes embedded controls which fix the access to the content to a specific device or set of devices.
12. The system according to Claim 1 wherein the content is encrypted.
20
13. The system according to Claim 1, wherein the permission wrapper includes embedded controls which limit the time frame in which the user can access the content.
- 25 14. A digital information security system for creating, archiving, transmitting and controlling archive content comprising:
- a. a first system on which content is created;
 - b. an archive including a permission wrapper having access controls and the
30 content stored therein;
 - c. means for transmitting the archive to a second system; and

- d. means for controlling the access and/or use of the content independent of the means for transmitting.

5 15. A method for controlling the access to and/or use of content in the form of digital information comprising the steps of:

- a. creating content;
- b. creating a permission wrapper which controls access to and/or use of the content;
- 10 c. placing the content and the permission wrapper into an archive;
- d. sending, by an original content provider, the archive to a first receiver;
- e. controlling, by the original content provider, the first receiver's access to and/or use of the permission wrapped content;
- f. sending, by the first receiver, the archive to a second receiver;
- 15 g. controlling, by the original content provider, the second receiver's access to and/or use of the permission wrapped content, wherein the control to the access and/or use by the second receiver is determined at the time the permission wrapper is created.

20 16. A server-less method for controlling the access to and/or use of content in the form of digital information comprising the steps of:

- a. creating content;
- b. transferring the content into an archive;
- 25 c. establishing varying levels of permission with respect to access to the content.

17. A secure container comprising content in the form of digital information and a permission wrapper having the ability to independently recognize threat levels.

30

18. A content protected permission wrapper comprising a variable portion which can adjust the permissions based on inputs from within the permission wrapper itself.
- 5 19. A secure content container including: content to be access and shared based on a content provider's permissions; an application capable of rendering the content; and a permission wrapper which can change its level of access based on input from outside the container.
- 10 20. A permission control wrapper which is used to protect digital information comprising:
- a. a means for creating an archive on any type of digital medium;
 - b. a means for assigning digital content to said archive;
 - 15 c. a means for assigning users their rights and access control permissions to said archive; and
 - d. a means for controlling user operations on said archive based on a license key that controls user accessible features of the permission wrapper.
- 20 21. A permission control wrapper as recited in Claim 20 further including a means for securely sharing content maintained in the archive to other users through email, on file servers and hard drives, and PC removable storage media.
- 25 22. A permission control wrapper as recited in Claim 20 further including a means for maintaining version control and synchronizing protected files and folders internal to archives and external with archives shared with other users.
- 30 23. A permission control wrapper as recited in Claim 20 further including a means of auditing user activity associated with the creation, sharing and use of files and folders protected in the archive.

24. A permission control wrapper as recited in Claim 20 further including a means of automatically changing the protection and permission controls of the archive based on associated threats to the data maintained inside.
- 5 25. A permission control wrapper as recited in Claim 20 wherein means for assigning include a means for saving and storing these user rights and access control permissions into common templates.
- 10 26. A permission control wrapper as recited in Claim 20 wherein said means for controlling include a means for automatically determining the protection requirements for said archive based on network connectivity state
- 15 27. The permission control wrapper as recited in Claim 20, which can be used to assign files to it computer operating system specific file operation commands, such as cut, paste, drag, drop, save as, and send to.
28. The permission control wrapper as recited in Claim 20, wherein the permission wrapper has the ability to hide the files and folders contained therein.
- 20 29. The permission control wrapper as recited in Claim 20, which can be used to provide permission control over all types of digital information, including: movie files, spreadsheets, music files, word processing files, database files, other types of entertainment content, presentations, and any other type of information that is stored in digital form.
- 25 30. The permission control wrapper as recited in Claim 20, which provides permission control features for assigning user access to files.
- 30 31. The permission control wrapper as recited in Claim 20, wherein the rights and access control permissions includes the ability to expire user access to content after a specific time interval or at a specific point in time.

32. The permission control wrapper as recited in Claim 20, wherein the rights and access control permissions includes the ability to change or modify files and folders maintained in the permission control wrapper.
- 5
33. The permission control wrapper as recited in Claim 20 wherein the rights and access control permissions includes the ability to add files and folders to the permission control wrapper.
- 10
34. The permission control wrapper as recited in Claim 20 which maintains and provides user templates in common groups of permission control for different levels of trusted users.
- 15
35. The permission control wrapper as recited in Claim 20 has embedded control features that provide the user with access to the content and the ability to perform operations on the protected content through a user interface, which control features are managed through a software license key that automatically allows or disallows user access to user interface control features that manage access to the archive.
- 20
36. The permission control wrapper as recited in Claim 20, wherein the user interface features controlled through the license key include user operations, which provides the ability to assign users to the content in the archive, and assigning those users their individual or group permission controls.
- 25
37. The permission control wrapper as recited in Claim 20, wherein the user interface features controlled through the license key include user operations, which include sharing operations, which provides the ability of the user to share content maintained in the archive through protected email, on all types of computer removable storage media, on hard drives and on file servers.

30

38. The permission control wrapper as recited in Claim 20, wherein the user interface features controlled through the license key include user operations, which include encryption operations, which provides the ability of the user to add files and folders to the permission wrapper in an encrypted form.
- 5
39. The permission control wrapper as recited in Claim 20, wherein the user interface features controlled through the license key include user operations, which include decryption operations, which provide the ability of the user to decrypt files from the archive and store them outside of the archive on all types of digital storage media, such as hard drives, computer removable storage media, disk arrays, etc.
- 10
40. The permission control wrapper as recited in Claim 20, wherein the user interface features controlled through the license key include user operations, which include audit operations, which provide the ability to recover user names and passwords, and access an event log of information maintained for the permission wrapper that tracks which users have access to the content, the type of access they are granted, when they were granted access to the content, on what devices are they allowed to access the content, the users that they in turn shared content with, and what operations the users have performed on protected files and folders maintained in the archive.
- 15
- 20
41. The permission control wrapper as recited in Claim 20, wherein the user interface features controlled through the license key include user operations, which include locking operations, which provide the ability to lock or fix the content in the archive to a machine, device or related group of machines and devices.
- 25
42. The permission control wrapper as recited in Claim 20, wherein the user interface features controlled through the license key include user operations, which include synchronization operations, which provide the ability to version control, update and synchronize files and folders with new information, and in turn to share those updates to other users that also have been granted access to the content through sharing operations.
- 30

- 5 43. The permission control wrapper as recited in Claim 20, wherein the user interface features controlled through the license key include user operations, which include view operations, which provide the ability to see the files and folders stored in the archive.
- 10 44. The permission control wrapper as recited in Claim 20, further including a means for securely sharing content maintained in the archive with other users through email, PDAs, instant messaging, on file servers and hard drives and PC removable storage media which provides users with secure sharing methods controlled functionally by the permission wrapper, and accessed through the user interface, which secure sharing methods ensure that the information remains in protected form not only during the actual sharing operation, but also when the content is installed and in use on a recipient's electric appliance.
- 15 45. The permission control wrapper as recited in Claim 20, which maintains version history of when files and folders have been added to the archive including all the repeat versions of files wherein the recognition of the latest version is based on the date stamp of the file assigned by the operating system.
- 20 46. The permission control wrapper as recited in Claim 20 which further includes an incremental update feature is provided by which a user may share only new or changed files with users that have access to protected files in the archive, said incremental update feature allows the user to only send the changed files, rather than
- 25 all of the files in the archive.
- 30 47. The permission control wrapper as recited in Claim 20 which further includes a synchronization feature which a user may notify other users of shared archives that a file or folder has changed, and those users may in turn receive only the updated or changed files or folders for shared content protected on their machines.

48. A permission control wrapper within an archive having protected content therein comprising a means for providing user access to the content in the archive based on embedded security policies.
- 5 49. The permission control wrapper as claimed in Claim 48 wherein said means for providing user access includes at least two of (i) a user permission model, (ii) a licensed feature set, (iii) a threat model and (iv) network connectivity state; and a means for recognizing the intersection of those items present in said means for providing.
- 10 50. A permission control wrapper which is used to protect digital information contained comprising:
- a. a means for creating an archive on any type of digital medium;
 - 15 b. a means for placing digital content into said archive;
 - c. a means for assigning users their rights and access control permissions to said archive;
 - d. a means for controlling user operations on said archive based on a license key that controls user accessible features of the permission wrapper; and
 - 20 e. a means for securely sharing content maintained in the archive with other users through a removable storage or digital media.
51. A permission control wrapper associated with an archive having protected content therein comprising a means of accessing the protected content through multiple
- 25 access methods including a graphical user interface, a batch or command line interface, and an application programming interface.
52. A permission control wrapper associated with an archive having protected content therein comprising means for hiding from a user at least a portion of the content
- 30 inside the archive, such portions cannot be directly executable upon by the direct operating system and application commands.

53. A permission control wrapper which is used to protect digital information comprising: a means for creating an archive on any type of digital medium including PD hard drives , file server drives, disk arrays, Personal Digital Assistants (PDAs),
5 recordable and rewritable CD and DVDs, Zip drives, tape storage devices, and all other types of computer medium that can be written to; a means for assigning digital content to said archive; a means for assigning users their rights and access control permissions to said archive; and a means for controlling user operations on said archive based on a license key that controls user accessible features of the permission
10 wrapper.

54. A system for controlling the access and/or use of protected content comprising a permission control wrapper including embedded security control policies, which policies are the rules by which the permission controls are enforced through the
15 permission control wrapper, said policies describe the allowable set of permissions that a user is granted based on an embedded table that defines the policies for users.

55. The system according to Claim 54 further including a means for enforcing said permissions based on the intersection of: a) the user trust level as assigned by the
20 Administrator of the archive, b) the network connectivity state of the user, c) the license key controlled feature sets for the user, which provides access to features of the permission wrapper through the user interface, d) whether or not a binding or locking restriction is associated with the user and e) if a threat has been detected on the user system on which the content is stored, the network segment that the user's
25 machine is located, or the pattern of the user behavior.

56. A system for controlling the access and use of protected content comprising a permission control wrapper that has the ability to understand the current state of user network access and automatically modifies the permission controls to be either more
30 or less restricted based on the recognition of whether or not the user is locally

connected to the network, remotely connected to the network, or disconnected from the network.

5

10

15

20

25

30